akt FOR WALLONIA

ECOLYS – 14 JUIN 2024

Cybersécurité
Un enjeu crucial pour votre PME

NOS INTERVENANTS

Charles CUVELLIEZ
Chief Information Security Officer
BELFIUS

Vincent DOCQ-CREMER
Gestionnaire Risques Opérationnels
CBC BANQUE

Lisa LOMBARDI
Experte Numérique
AKT FOR WALLONIA (UWE)

Bertrand MASSET
Manager Ethical Hacking
APPROACH

Débat animé par :

Amid FALJAOUI
Directeur de
TRENDS-TENDANCES

En collaboration avec :

Belfius CBC

Avis aux participants : Prise de photos et/ou vidéos

- **Attention !** Des photos et vidéos pourraient être prises pendant cet événement.
- Les photos et vidéos prises pendant l'événement pourraient être utilisées à des fins promotionnelles ou de communication par les organisateurs pendant une période de deux ans.
- Vous avez le droit de demander que vos photos ou vidéos soient retirées de tout support public.
- Les organisateurs s'engagent à respecter votre vie privée et à ne pas diffuser d'images ou de vidéos vous concernant si vous vous y opposez.
- **En participant à cet événement, vous acceptez que votre image puisse être prise et utilisée conformément à ces directives.**
- Si vous ne souhaitez pas que votre image soit utilisée, veuillez en informer un membre de l'organisation dès que possible.
- **Si vous avez des questions ou des inquiétudes, n'hésitez pas à contacter un membre de l'organisation ou à nous adresser votre message par email à <privacy@uwe.be>.**
- Veuillez noter que notre politique de vie privée est consultable sur: https://www.uwe.be/politique-de-vie-privee/
- Nous vous remercions de votre compréhension.

Agenda

- 12h00 : Accueil sandwiches
- 12h20 : Mots de bienvenue
- 12h25 : Démonstration live d'un hacking éthique par **Bertrand Masset**, Manager Ethical Hacking chez Approach Cyber
- 12h45 : Table-ronde animée par **Amid Faljaoui** en présence de :
    - **Charles Cuvelliez**, Chief Information Security Officer chez Belfius
    - **Vincent Docq-Cremer**, Gestionnaire Risques Opérationnels chez CBC Banque
    - **Lisa Lombardi**, Senior Advisor chez AKT for Wallonia (UWE)
- 13h30 : Networking
- 14h00 : Fin

ECOLYS – 14 JUIN 2024

akt

Belfius

CBC

AKT aujourd'hui

ASBL indépendante,
représentant les entreprises,
de la startup à la multinationale,
quel que soit le secteur d'activités

24
FÉDÉRATIONS SECTORIELLES

> de 80.000
ENTREPRISES DÉFENDUES

2/3
EMPLOI PRIVÉ

1
ÉQUIPE D'EXPERTS ENGAGÉE AU SERVICE DES MEMBRES

+ de 22.000
FOLLOWERS RÉSEAUX SOCIAUX

SDG
VOICE 2020

4 grandes priorités pour une prospérité territoriale et sociétale

01

EMPLOI – FORMATION

Un taux d'emploi de 80%

02

ENVIRONNEMENT - CLIMAT

Une Wallonie qui atteint ses objectifs climatiques et environnementaux

03

INNOVATION – INVESTISSEMENT

Une industrie compétitive, y compris à l'exportation, sur base de sa productivité et de son degré d'innovation

04

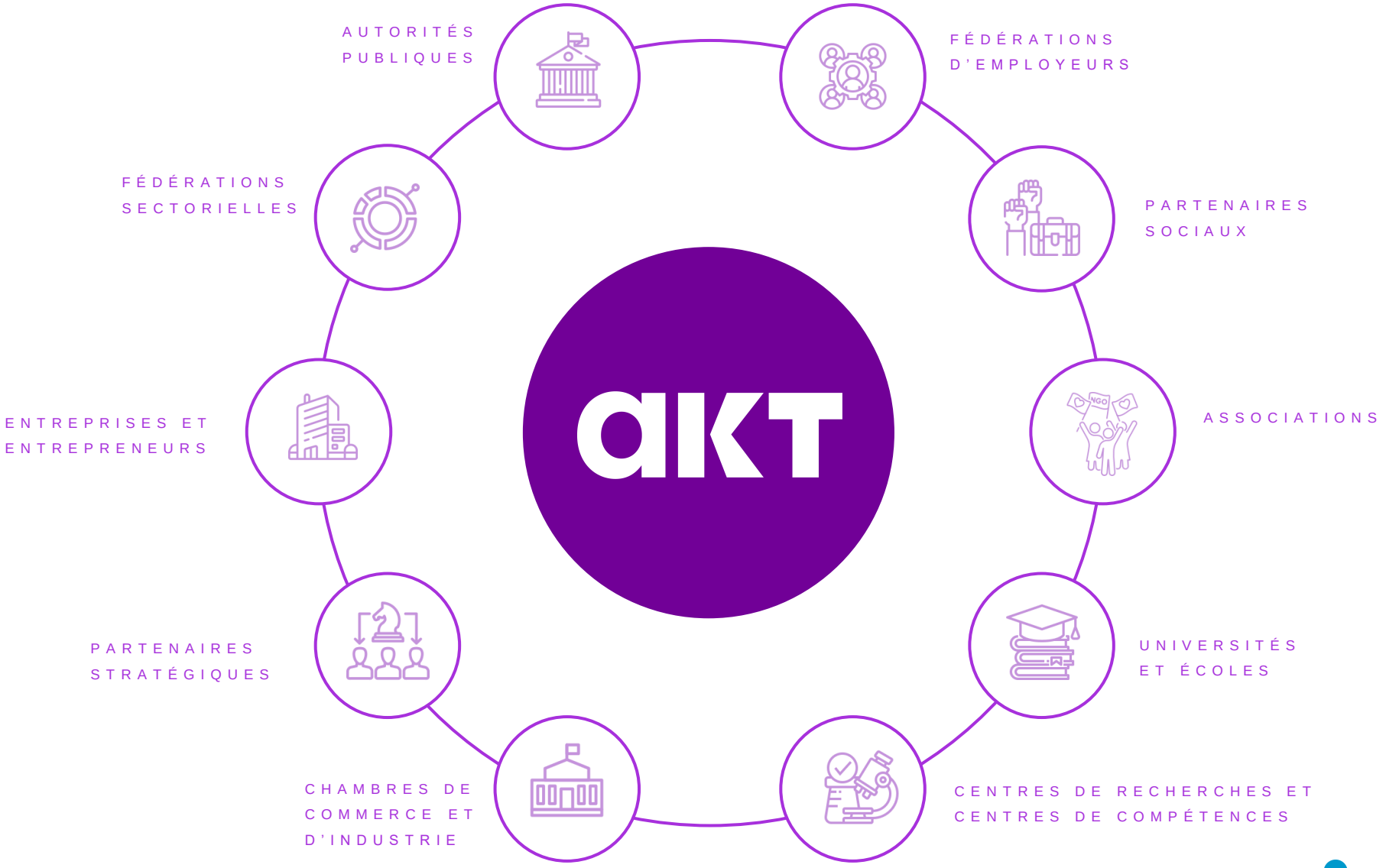
GOUVERNANCE - ADMINISTRATION

Une administration efficiente au service de ses usagers, en symbiose avec un gouvernement dont les actions sont guidées par des indicateurs transparents

PROSPÉRITÉ TERRITORIALE ET SOCIÉTALE

Au cœur de l'écosystème

AKT for Wallonia se positionne au cœur du paysage économique wallon, connectée avec tous les acteurs qui comptent pour accélérer la dynamique de création et de développement des entreprises



Introduction

Cécile NEVEN
CEO
AKT FOR WALLONIA

01

Démonstration live d’un hacking éthique

Bertrand MASSET
Manager Ethical Hacking
APPROACH CYBER

02

03

Table-ronde

CYBERSÉCURITÉ: UN ENJEU POUR VOTRE PME

Table-ronde animée par Amid FALJAOUI

Charles CUVELLIEZ
Belfius

Vincent DOCQ-CREMER
CBC

Lisa LOMBARDI
AKT for Wallonia

Quelques chiffres clés

92

% des attaques commencent avec un phishing

650

Nombre de cyberattaques sur des entreprises par semaine en Belgique

38

% des cyberattaques entraînent un arrêt d'activité pour l'entreprise

3

Si la cybercriminalité était un pays, ce serait la 3ème économie mondiale

>50

% de toutes les cyberattaques visent les PME

> de 100.000

€ de dommages pour 1 préjudice sur 5

Sources:

- Cyberwal by Digital Wallonia
- Center for Cybersecurity Belgium (CCB)
- Statistica
- Statistiques et Cibles de la Cybersécurité en 2024 ! (techopedia.com)

Axel LEGAY, Professeur, UCLouvain

« Il faut en Europe et en Wallonie une approche de la cybersécurité identique à celle des US. Là, plus votre entreprise est protégée, plus c'est positif pour votre réputation et plus votre entreprise a de la valeur ».

CYBERSÉCURITÉ:
UN ENJEU
CRUCIAL POUR
VOTRE PME

4 grands défis pour les entreprises wallonnes

01

CONTEXTE INTERNATIONAL

La sophistication et la mondialisation des cyberattaques

02

DIGITALISATION CROISSANTE

Explosion des applications sur et en-dehors du réseau de l'entreprise, travail hybride, développement de l'IoT, …

03

INVESTISSEMENT

Manque de compétences internes et de ressources suffisantes dans le chef de nombreuses PME

04

RÉGLEMENTATION

Evolution des règles de conformité

Frédéric WILQUEM, Aerospace & IS Specialist

« Un risque auquel plus aucune entreprise n'échappe aujourd'hui, mais aussi une opportunité pour chacune d'entre elles de se démarquer de ses concurrents !"

CYBERSÉCURITÉ: UN ENJEU CRUCIAL POUR VOTRE PME

La cybersécurité, une question de gouvernance

01

- Intégrer la préoccupation cyber dans la stratégie globale de l'entreprise
- Démontrer un engagement personnel du dirigeant
- Définir les rôles et responsabilités
- Encourager les remontées d’anomalies
- Encourager les collaborateurs à être prudents
- Se conformer par rapport aux lois et réglementations
- S'assurer que la cybersécurité est régulièrement évaluée, mise à jour et communiquée à tous les niveaux de l'organisation
- Penser aux assurances contre les cyber-risques
- Investir dans la formation des collaborateurs
- Diffuser les bonnes pratiques d’hygiène numérique

David VANDEROOST, CEO, Approach Cyber

« Avec la nouvelle loi NIS2, les dirigeants et les membres du conseil d'administration deviennent personnellement responsables et s'exposent à des sanctions en cas de négligence dans la gestion des risques cyber ».

NIS 2 : nouvelle directive européenne sur la cybersécurité

- La loi NIS2 est LE sujet de conformité de l'année 2024
- De nombreux secteurs et entreprises sont concernés
- Notamment les entreprises d'une certaine taille (à partir de taille « moyenne »), dans les secteurs critiques et importants pour la résilience de la société en général
- Les petites sociétés sont aussi indirectement touchées – elles sont souvent impliquées dans la chaine d'approvisionnement des entités concernées par NIS2

CYBERSÉCURITÉ: UN ENJEU CRUCIAL POUR VOTRE PME

La cybersécurité, une question de bonnes habitudes numériques

02

- Veiller à l'obsolescence du matériel informatique
- Mettre à jour régulièrement les logiciels et les systèmes
- Sécuriser et gérer les identités
- Activer l'authentification forte et les *Conditional Access Policies*
- Activer l'authentification multifacteur (MFA)
- Faciliter le single sign-on et le contrôle d'accès à toutes les applications et données
- Mettre en place une solution de gestion des risques et de réduction de la surface d'attaque:
  - Sauvegardes (backup 3-2-1-1-0 + Encryption & Data Loss Prevention)
  - Cloisonnements des réseaux
  - Limitations des accès utilisateurs, …

ADOPTER UNE POSTURE PRÉVENTIVE POUR ÉVITER QUE LES ATTAQUES NE SE PRODUISENT

CYBERSÉCURITÉ: UN ENJEU CRUCIAL POUR VOTRE PME

La cybersécurité, une question de spécialistes

03

- Évaluer continuellement les accès pour remédier en temps réel à une compromission potentielle
- Effectuer des exercices réguliers de prévention
- Effectuer une réflexion sur les actifs les plus essentiels à protéger au sein de l'entreprise
- Mettre en place un plan de réponse aux incidents
- Préparer un plan de continuité en cas d'attaque
- Réaliser un audit de sa cybersécurité
- Effectuer des tests d'intrusion (pentests) afin de détecter les vulnérabilités potentiellement exploitables et y remédier

LES CYBERCRIMINELS SONT DES PROFESSIONNELS, VOTRE CYBERSÉCURITÉ DOIT L'ÊTRE AUSSI

Eric VAN CANGH, Senior Business Group Leader Digital, Agoria

« Si l'entreprise n'a pas la connaissance ou la capacité structurelle ou humaine de mettre en place une politique de cybersécurité adaptée, il est impératif de se faire conseiller ou d'externaliser certaines activités ».

KEY TAKEAWAYS

3 conseils de mise en action

N’attendez pas

- Il est crucial d'établir rapidement un plan de cybersécurité solide et de le communiquer efficacement au sein de l'organisation.
- Si vous n’avez pas encore de plan de sécurité en place dans votre entreprise, vous vous exposez à des risques significatifs, en termes de continuité, et de conformité.
- Le cadre légal évolue rapidement sous la pression de l’Union Européenne. N’attendez ni les pirates, ni les sanctions légales du régulateur.

Investissez dans la formation et la sensibilisation

- (In)Formez-vous et formez régulièrement vos employés aux bonnes pratiques de cybersécurité, notamment en matière de gestion des mots de passe, de reconnaissance des emails de phishing et de manipulation des données sensibles.
- Il existe des solutions innovantes pour entrainer et former vos collaborateurs.

Établissez des partenariats avec l'écosystème cyber

- Collaborez avec les acteurs clés de l'écosystème cyber en Belgique et en Wallonie, tels que les associations professionnelles, les autorités régionales et les consultants en cybersécurité.
- Ces partenariats offrent un accès à des conseils spécialisés, à des ressources techniques avancées et à des informations sur les menaces actuelles, et des soutiens financiers, ce qui est essentiel pour maintenir une cybersécurité robuste face aux évolutions rapides du paysage cyber.

Avec le soutien d’Approach Cyber

Ressources utiles

Belfius

Devenez CYBER Smart

- **Les TRUCS et ASTUCES de Belfius pour reconnaître et prévenir la fraude :**

https://www.belfius.be/fraude

- **Un doute ou une question? Contactez votre personne de contact habituelle (Banker/Servicing Officer)**
- **En cas d’urgence ou de fraude avérée:**

Appelez Belfius Fraud Stop (24h24): 02 222 46 00

Ressources utiles

- **Informations à destination des clients de CBC**

Déjouez les arnaques liées aux services bancaires - CBC Banque et Assurance

https://www.cbc.be/particuliers/fr/info/secure4u/dossier-fraude.html

- **Guide pratique pour PME réalisé par la Cyber Security Coalition dont CBC fait partie**
- **https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-guide-sme-FR.pdf**

https://www.cybersecuritycoalition.be/

Ressources utiles

.AGORIA

La fédération de l'industrie technologique, regroupe 2079 entreprises technologiques et tous ceux qui sont inspirés par la technologie.

- **Services et expertise en matière de cybersécurité:**

https://www.agoria.be/fr/services/expertise/digitisation/cybersecurity/services/conseil-cybersecurite

- **Programme d'accompagnement CyberStart** :

https://www.agoria.be/cyberstart/fr

- **Programme WalHub dédié aux PME manufacturières** :

https://www.walhub.be/fr/

#études #événements #groupesdetravail #services #expertise #réseautage #conseil

https://www.agoria.be

Ressources utiles

Cyberwal by digital wallonia

Le programme régional public wallon pour la cybersécurité dont AKT for Wallonia pilote l'axe « Sensibilisation & Accompagnement »

Il fédère les acteurs wallons de la cybersécurité, dans le domaine de la recherche, de l'innovation et de la formation.

https://www.digitalwallonia.be/cyberwal

#chiffresclés #événements #livresblancs #articles #vidéos

- **Boîte à outils de cybersécurité pour petites entreprises**

https://gcatoolkit.org/fr/petites-entreprises

+

- **Outil de mesure de la maturité numérique**

https://digiscore.digitalwallonia.be/

€ Ressources utiles

Chèques-entreprises

- **Les chèques cybersécurité dont peuvent bénéficier toutes les PME wallonnes:**

https://www.cheques-entreprises.be/cheques/cybersecurite

Le Chèque-cybersécurité permet de vous faire aider par un spécialiste pour réaliser un audit ou un diagnostic portant sur la situation de votre entreprise en termes de cybersécurité.

Ce consultant, ou un autre, pourra ensuite prendre le relais pour mettre en place les actions préconisées dans le cadre de l'audit ou du diagnostic cybersécurité.

75% d'intervention | Maximum 50000€ htva sur 3 ans

CENTRE FOR
CYBERSECURITY
BELGIUM

Ressources utiles

L’autorité nationale en charge de la cybersécurité en Belgique. Il supervise, coordonne et veille à la mise en œuvre de la stratégie belge en matière de cybersécurité.

- **L'outil CyFun niveau « Basic »**

34 contrôles et 8 mesures-clés pour vous protéger de 82% des cyberattaques :

https://ccb.belgium.be/sites/default/files/cyberfundamentals/CYFUN_BASIC_FR_20230301.pdf

- **Informations sur la Directive NIS2:**

https://ccb.belgium.be/fr/article-tags/nis2

#études #expertise #outils

https://ccb.belgium.be/fr

Ressources utiles

- **Safe on Web at Work**

Pour signaler un problème, passer le test de cybersécurité ou recevoir des conseils pratiques:

https://atwork.safeonweb.be/

- **La Cyber Emergency Response Team fédérale (CERT.be)**

Service opérationnel du CCB chargé de détecter, d'observer et d'analyser les problèmes de sécurité en ligne et d'informer la population à ce propos:

https://ccb.belgium.be/fr/cert

Ressources utiles

APPROACH CYBER

- **Guide de préparation à NIS2 mis à disposition par Approach Cyber**

https://www.approach-cyber.com/en/publications/nis2-directive-strengthening-cyber-security-europe.html

Approach Cyber vous aide à naviguer dans la nouvelle législation visant à renforcer la cybersécurité en Europe, et à prendre les mesures adéquates pour vous y conformer rapidement.

Ressources utiles

VBO FEB
Verbond van Belgische Ondernemingen
Fédération des Entreprises de Belgique

- **La Cyberincident Roadmap développée par la FEB :**

  https://www.feb.be/publications/cyber-incident-roadmap/

  L'objectif de cette roadmap est d'aider les entreprises victimes d'un cyberincident dans leur organisation en interne, mais surtout de les aider dans leur interaction avec leurs contacts externes, notamment les autorités publiques, et ce, dans le cadre de leurs obligations légales.

Ressources utiles

- **Conseils pratiques (brochures, vidéos, …) du secteur bancaire belge**

Fraude et sécurité · Types de fraudes en ligne · Fraude offline · Mules financières · Criminalité financière, blanchiment d'argent et financement du terrorisme…

https://febelfin.be/fr/themes/fraude-et-securite/fraude-aux-paiements-et-entreprises

.

MERCI POUR VOTRE PARTICIPATION!

Des questions? Nos experts sont là pour y répondre

Bertrand MASSET

Ethical Hacking Manager

Approach Cyber

bertrand.masset@approach-cyber.com

https://www.approach-cyber.com/

https://www.linkedin.com/in/bertrandmasset/

Charles CUVELLIEZ

Chief Information Security Officer

Belfius

https://www.belfius.be

https://www.linkedin.com/in/charles-cuvellliez2/

Vincent DOCQ-CREMER

Gestionnaire de Risques Opérationnels

CBC Banque

https://www.cbc.be

https://www.linkedin.com/in/vincent-dc-2b14526/

Lisa LOMBARDI

Senior Advisor

AKT for Wallonia

Lisa.Lombardi@uwe.be

https://www.uwe.be

https://www.linkedin.com/in/lisalombardi/

MERCI POUR VOTRE PARTICIPATION!

akt

Belfius

CBC

WWW.UWE.BE